EXPLORING CYBERSPACE WITHOUT FEAR

Our nation invests billions of dollars annually discovering, developing, and deploying advanced technology. This technology is the critical enabler of the powerful and precise capabilities our military now enjoys– and our forces rely on these capabilities to accomplish their mission. Our enemies understand this and attempt to exploit our capabilities by acquiring critical DoD technology. Historical evidence indicates that unprotected technology is easily stolen and replicated. Whatever your organization's role in developing critical technology, the ATSPI Technology Office can assist you in identifying your critical technology and provide protection solutions tailored to the value of the Intellectual Property and your specific use case.

ATSPI Technology Office

AFRL/RYT

2241 Avionics Circle

WPAFB, OH 45433-7320

(937) 320-9095 x150

AT-SPI_outreach@wpafb.af.mil

http://spi.dod.mil

Sponsored by:

HPC Modernization Program

Deputy Under Secretary for Defense Science & Technology

28 November 2007 PA # WPAFB-07-0557

SOFTWARE PROTECTION INITIATIVE

http://spi.dod.mil

IDENTIFYING AND PROTECTING CRITICAL INTELLECTUAL PROPERTY

SAFE COLLABORATION THROUGH TECHNOLOGY

SPI MISSION:

MARGINALIZE A NATION-STATE CLASS THREAT'S ABILITY TO STEAL AND EXPLOIT CRITICAL DOD INTELLECTUAL PROPERTY FOUND IN APPLICATION SOFTWARE.

The SPI Program, established by USD (AT&L), was founded on the principal focus to protect critical DoD intellectual property (ostensibly application software including executables, source code, and data) from piracy, tamper, and exploitation by nation-state class threats.

The SPI Program addresses the need of an alternative approach to implementing security in depth for Information Technology (IT) systems that will provide cost effective defenses against nation-state class threats and can be built from commercial components available today.

THREAT-DRIVEN SOLUTIONS

- Anti-Piracy - Protected development, distribution, and execution
- Code Integrity - Trusted execution
- Anti-Reverse Engineering - Intellectual Property (IP) protection

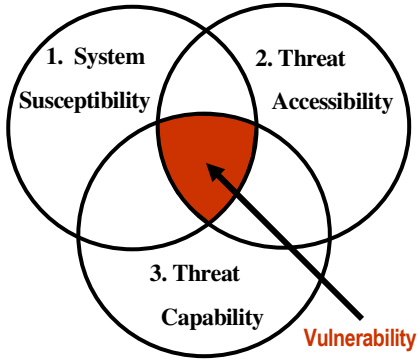
EXAMPLES OF CRITICAL APPLICATION SOFTWARE

- Science & Engineering/Modeling & Simulation Software
- Mission Support Software running on COTS
- Enterprise Software

SPI TENETS:

PRODUCING IT SECURITY SYSTEMS THAT ALLEVIATE THREATS WHILE BEING COMPATIBLE WITH DOD IT SYSTEMS.

1. **Reduce scope of IT system susceptibility**: identify technology critical to protect and eliminate reliance on security elements that can't be trusted.
2. **Make critical items inaccessible to the threat**: move intellectual property and trusted security elements "out-of-band".
3. **Shrink threat capability through use of Detect & React security elements**: deny attack tools autonomously, stay inside the threat's OODA loop, and impose hard penalties.



Use "COTS parts with government smarts" to shrink adversary's playing field.

THREATS TO DOD IP: RECENT HEADLINES

- Pentagon shuts down systems after cyber-attack: 1500 computers taken offline due to a breach within the Office of the Secretary of Defense. PC WORLD
- Homeland Security computers hacked: Information moved from Homeland Security computers to Chinese language websites. CNN
- Chinese hackers seek U.S. access: Concerns about the security of the internet's infrastructure deepen after the cyber attack of a U.S. military computer system. USA TODAY

SPI PRODUCTS

- **Cyber Sensing Station (CSS)**
  - Secure enclave for collaboration
  - Freedom for researchers to configure each system as desired
  - Isolates user systems from threat
  - Outsider attack prevented through TPCI modules and hardware level encryption

- **Mobile Solutions**
  - ICEBox
  - Light-weight Portable Security (LPS)
  - Browser On a Stick

- **Secure Application Sharing**
  - Secure Launcher
  - Code Server with Crypto Aware Editors and compilers
  - Encryption Wizard

Does my code need protection?

SPI has developed the CPI/CT Tool to help program managers identify program specific critical technologies.

CPI/CT Tool